

# ATTACHMENT A

## UNITED STATES DISTRICT COURT

for the  
Middle District of Tennessee

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Premises known as  
DR. GILBERT GHEARING FAMILY MEDICINE AND  
OBSTETRICS 151 McArthur Avenue, Celina, TN 38551

Case No.

19-MJ-2216

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Middle District of Tennessee, there is now concealed (identify the person or describe the property to be seized):

See Attachment B and D.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 841 and 846	Unlawful Dispensing of Controlled Substances and Conspiracy to Violate
18 U.S.C. 1347 and 1349	Health Care Fraud and Conspiracy to Violate; and Title 42 Anti-kickback Statute
18 U.S.C. 1956 and 1957	Money Laundering

The application is based on these facts:

See attached Affidavit, at Attachment C pages 1-43.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

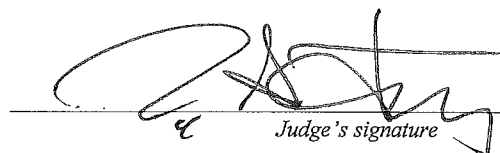
Thomas D. Esslinger, Special Agent, DEA

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/07/2019

City and state: Nashville, Tennessee



Judge's signature

Judge Jeffrey S. Frensley, U.S. Magistrate Judge

Printed name and title

## ATTACHMENT A

### PROPERTY TO BE SEARCHED

#### TARGET LOCATION

DR. GILBERT GHEARING FAMILY MEDICINE AND OBSTETRICS is located at 151 McArthur Avenue, Celina, Tennessee 38551. It is a reddish-brown, one-story brick building. It is currently being used as a duplex, and the clinic occupies the left half of the building. The other half is occupied by Anderson Hometown Pharmacy. The main entrance to the clinic is a glass door and has a store sign "Ghearing MD" painted on the main entrance door. There is a ramp walkway with railings from the front parking lot to the main entrance door. A photo of the location is depicted below.



## **ATTACHMENT B**

### **DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**

The search of the property described in Attachment A shall include all records, documents, materials, and information, whether found in physical, electronic/digital format, magnetic, or optical, for the time period of December 2015 to the present, that may constitute fruits, evidence, information, contraband or instrumentalities, in whatever form and however stored, relating to criminal violations of Title 21, United States Code, Sections 841 (Illegal Distribution and Dispensing of Controlled Substances) and 846 (Conspiracy to Distribute and Dispense Controlled Substances), Title 18 United States Code, Sections 1347 (Health Care Fraud), 1349 (Conspiracy), Sections 1956 and 1957 (Money Laundering), and 42 U.S.C. § 1320a-7(b) (Anti-Kickback Statute), based on acts relating to GHEARING, his employees, agents, designees, co-conspirators or aiders and abettors. These items include, but are not limited to:

1. All documents, records, communications, and correspondence relating to controlled substances and non-controlled medications.
2. Computers, digital devices, and electronic evidence, as described in the warrant and to be searched and seized in the manner and means described in the warrant, including records and information relating to contact lists, call logs, e-mails, SMS, MMS, internet history, applications, notes, or voicemails on the cellular telephones/smartphones with internet access used in connection with the referenced offenses and individuals and entities.
3. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically-stored material that explains or illustrates the configuration or use of



any seized computer hardware, software, or related items, system documentation, and software and instruction manuals.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, or destruction of any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form, and any evidence eliminator or data wiping software.
6. Any and all documents and records of activities relating to the operation of a computer, notes (however and wherever written, stored or maintained), books, diaries, and reference materials, and any and all notes or records relating to such items containing information pertaining to them, including but not limited to file names, user names, passwords, telephone numbers, and access devices, together with indicia of use, ownership, possession, or control of such records.
7. Printers, facsimile machines, copiers, typewriters, or other devices capable of being used in the creation of the documents described in this affidavit.
8. Any and all correspondence, records, notes, documents, statements, cancelled checks, wire transfers, sales receipts, invoices, bills, checkbook registers, financial documents, or other materials of any kind, relating to any bank accounts, whether personal or business accounts, investment accounts, financial accounts, loans, personal identifying information, and business activity. This specifically includes, but is not limited to, correspondence, records, notes, documents, statements, cancelled checks, checkbook registers, and related materials.
9. Any and all documents and records of communications and/or transactions with entities providing services to the medical office of GHEARING or acting as pass-through entities for such services.
10. Any and all of the following items related to the medical practice of GHEARING:
  - a. Any and all Medicaid, Medicare, TriCare, or any Private Health Insurance Company enrollment applications, electronic funds transfer agreements, electronic data interchange agreements, manuals, documents, contracts, bulletins, instructions, and correspondence relating to these entities.
  - b. Any and all claims, cost reports, or other insurance information regarding claims submitted, including, but not limited to, Medicare, Tennessee Medicaid/TennCare, TriCare and/or any Private Health Insurance Company, including, but not limited to, all documents, invoices, worksheets,

communications, memorandums regarding the preparation and submission of cost reports or claims of any kind to Medicare, Tennessee Medicaid/TennCare, TriCare or Private Health Insurance Company, in whatever form – electronic or paper;

- c. Any and all patient medical records and patient files in whatever form – electronic or paper – for the individuals listed in Attachment D. Patient files and medical records include any and all information relating to medical services or items provided to patients, including but not limited to, the following: referring physician forms, physician's orders and prescriptions, progress notes, patient biographical data, receipts of payments or co-pays for patient visits, medical or diagnostic test orders and results, notes regarding office visits, patient sign-in sheets, intake sheets, authorization forms, Certificates of Medical Necessity, face sheets, correspondence, coinsurance information, insurance verification forms, copies of patient identification documents and insurance cards, appointment notices and receipts, and any documentary information, including internal notes, identifying or otherwise discussing the medications and/or services provided to a particular patient and the corresponding prescribing doctor, employee or entity.
- d. Any and all information and documentation relating to the writing of prescriptions for controlled substances, and other medications, including prescription pads and inventories;
- e. Any and all information relating to patient urine screenings, including, but not limited to, patient information, testing and results, and billing.
- f. All patient lists, including appointment books, calendars, and sign-in sheets;
- g. Any and all Health Care Insurance billing/payment records, including, but not limited to, provider/supplier remittance advices, claims for services provided, and Health Care Insurance payment checks;
- h. Any and all patient complaints, audits, or medical reviews of GHEARING or entities affiliated or associated with him;
- i. Appointment books, calendars, sign-in sheets of any associated practitioner or employee working for or at the direction of GHEARING;
- j. Any and all documents, notes, reports, charts, analysis, graphs, letters, memoranda, email, text message, instant message, proforma reports, estimates, contracts (including all attachments) or agreements involving or relating to referrals of patients to any company, entity or individual;
- k. Any and all owner, manager, or employee files or documentation of GHEARING, including, but not limited to, any information showing any ownership, licenses, accreditations, or training completed by GHEARING or employees working for or at the direction of GHEARING;

- l. Any and all contracts, agreements, or correspondence between GHEARING or employees working for or at the direction of GHEARING and health laboratories and third-party healthcare providers, such as pharmacies, including, but not limited to, purchase agreements, leases, management agreements, lease agreements, contracts, due diligence reports/documents, etc.;
  - m. Any and all information and documentation regarding management meetings, agendas, notes, documents, or board of director meeting minutes, notes or recordings;
  - n. Training materials, manuals, employee handbooks, standard operating procedures, marketing materials, advertisements, and policies and directives regarding the operation of GHEARING's medical clinic;
  - o. Complete employee personnel files;
  - p. Any and all documentation and information regarding the ownership of GHEARING's medical practice, the building of the TARGET LOCATION or entities associated with GHEARING;
  - q. Any and all information and documentation related to including compensation of GHEARING, anyone working at the direction of GHEARING or any individuals or entities associated with GHEARING; and
  - r. Any and all contracts/leases/agreements relating to or associated with the medical practice of GHEARING with any vendor or provider of services, including details regarding invoices and compensation.
11. Any and all contracts, agreements (including independent contractor agreements, consulting agreements, compensation agreements, stock option agreements, etc.), memoranda of understanding, billing statements, invoices, loan statements, receipts, marketing material, or written materials of any kind indicating the purchase of goods and/or services by, and/or the business or financial practices of GHEARING.
12. All accounting, bookkeeping and financial records relating to receipts and expenditures including bank accounts, bank statements, credit card statement, records of accounts, records of income, journals, ledgers, financial statements, balance sheets, trial balances, statements of profits and losses, accounts and notes receivable, accounts and notes payable, check registers and canceled checks, cashier checks, wire transfer confirmations, federal, state and local income tax returns including all schedules and attachments for drafts and filed returns, work papers, notes and memoranda, all tax records including tax preparation files, and documents relating to all other governmental filings or public statements relating to GHEARING.

13. Records, envelopes (whether opened or unopened), letters, correspondence, electronic mail (whether opened or unopened), chat logs, instant messages, faxes, and log files, and any and all computer storage media, which concerns or relates to:
  - a. Correspondence, communication, or agreements by, among, or related to, any individuals that worked for, or have a financial interest in the medical practice of GHEARING;
  - b. Any evidence establishing use, control, or access to any and all computer systems found in the locations subject to search;
  - c. Any and all passwords or commands that control access to any computer, files, or data; and
  - d. Any and all files, log files, data files and records relating to the use of internet service providers for purposes of committing the criminal offenses listed above.
14. Any and all payroll records, paycheck stubs, receipts, Forms K-1, or other documents or papers of any kind relating to any income earned, and/or expenses accrued, by any individuals and/or entities, including their employees, of GHEARING.
15. All United States Information Returns (i.e. Forms 1096 and 1099), United States Individual Income Tax Returns (Form 1040), United States Corporation Income Tax Returns (Forms 1120 and 1120S), United States Partnership Income Tax Returns (Form 1065), Wage and Tax Statements (Form W-2), Employer's Quarterly Federal Tax Returns (Form 941), and Employer's Annual Federal Unemployment Tax Returns (Form 940) and information and documentation related to tax filings for any business associated with or relating to GHEARING.
16. Any photographic, video, or audio recordings of conversations and/or other activities related to the TARGET LOCATION.
17. Any safe, strongbox, lockbox, and/or other container used, designed, or intended to secrete or secure valuables and/or property from disclosure or taking, including keys, combinations, and any and all documents and records relating thereto.
18. All documents relating to any and all transactions involving the proceeds of financial transactions, including, but not limited to, purchases and/or acquisitions of real and personal property including real estate, homes, commercial buildings, aircraft, vehicles, jewelry, stocks, bonds, mutual funds, precious stones and metals, and any and all other articles of significant intrinsic value.
19. Documents or records indicative of the place of purchase, purchase price, method of payment, source of purchase funding, or ownership for all items of value, whose purchase price or fair market value could reasonably be believed to be in excess of \$100.



20. Any and all documents and records relating to current and former employees, including any and all personnel information, names and identifying information, payroll records, and training records.
21. All documents referring or relating to any 401(k) plan or trusts, including, but not limited to, any statements, records, orders, and communications and/or agreements with the Plan Administrator, Trustee, or Executor.
22. All calendars, appointment books, diaries, planners and contacts lists or address books.
23. United States Currency.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

All records seized will be retained in a secure location in order to protect patient confidentiality. Patient information seized during the execution of this search warrant that is covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164) will be protected and kept confidential as required by law; access to such information will be limited to those individuals necessary for the investigation or prosecution of this matter.

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF:  
  
Premises Known As DR. GILBERT GHEARING  
FAMILY MEDICINE AND OBSTETRICS 151  
McArthur Avenue, Celina, TN 38551

Case No. 3:18-mj-\_\_\_\_\_

**19-MJ-2216**

**Filed Under Seal**

**ATTACHMENT C**  
**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

Your affiant Tom Esslinger, being duly sworn, deposes and states as follows:

**IDENTITY AND EXPERIENCE OF AFFIANT**

1. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 21 of the United States Code, who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 21. I am presently employed as a Special Agent (“SA”) for the United States Drug Enforcement Administration (“DEA”), and have been so employed for approximately fourteen (14) years. In that role, I am responsible for investigating crimes that involve unlawful importation and exportation of controlled substances, the possession with the intent to distribute controlled substances, the distribution of controlled substances, the use of communication facilities to further these offenses, as well as the related laundering of monetary instruments, in violation of Title 21, United States Code, Sections 841 (Illegal Distribution and Dispensing of Controlled Substances), 846 (Conspiracy to Distribute and Dispense Controlled Substances); and violations of Title 18, United States Code, Sections 1347 (Health Care Fraud), 1349 (Conspiracy to Commit Healthcare Fraud), 1956 and 1957 (Money Laundering), and Title

42, United States Code, Section 1320a-7(b) (Anti-Kickback Statute). I am currently assigned to the Nashville District Office – Tactical Diversion Squad. The Tactical Diversion Squad is tasked solely with the investigation of the illegal trafficking of pharmaceutical controlled substances.

2. I have specialized training and experience in narcotics trafficking, conspiracy, and distribution investigations. I have participated in all aspects of drug investigations, including the use of confidential sources and undercover officers, physical surveillance, electronic surveillance, the execution of search and arrest warrants, the use of court-ordered intercepts of electronic communications, investigative interviews, the arrests of drug traffickers, and the analysis of seized records, physical evidence, and taped conversations. I have spoken on numerous occasions with other experienced narcotics investigators concerning the methods and practices of drug traffickers. In addition, I have consulted with physicians as expert witnesses, reviewed prescription records and patient medical files, and have spoken with witnesses having extensive knowledge of pharmaceuticals and the methods and practices of individuals trafficking in or diverting pharmaceutical controlled substances.

3. Through my investigations, my training and experience, and my conversations with other law enforcement personnel, I have become familiar with the tactics and methods used by traffickers to smuggle and safeguard pharmaceutical controlled substances, to distribute and divert pharmaceutical controlled substances, and to collect and launder the proceeds from the sale of controlled substances. Further, I am aware of the tactics and methods employed by pharmaceutical trafficking organizations and individuals to thwart investigation of their illegal activities.

#### **PURPOSE OF THE AFFIDAVIT AND TARGET LOCATION**

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known and described as the medical office of Dr. Gilbert Ross Ghearing (“GHEARING”), located at 151 McArthur Avenue, Celina,

Tennessee 38551 ("TARGET LOCATION"), more particularly described in the following paragraphs and in Attachment A for evidence, contraband, instrumentalities, and fruits of crimes, as further described in the following paragraphs and particularly in Attachment B, and to seize evidence, instrumentalities, contraband and fruits of crimes of GHEARING and any co-conspirators.

5. Based on my training, experience, and facts as set forth in this Affidavit, there is probable cause to believe that GHEARING, and others known and unknown to the investigation, have committed violations of Title 21, United States Code, Sections 841 (Illegal Distribution and Dispensing of Controlled Substances) and 846 (Conspiracy to Distribute and Dispense Controlled Substances); violations of Title 18, United States Code, Sections 1347 (Health Care Fraud) and 1956 and 1957 (Money Laundering); and Title 42, United States Code, Section 1320a-7(b) (Anti-Kickback Statute). Based on the same, probable cause also exists to search the TARGET LOCATION (more particularly described below and as set forth in Attachment A), for evidence, instrumentalities, and fruits of these crimes, as further described in Attachment B.

6. All of the information contained in this affidavit is based on my personal knowledge and observations during the course of this investigation, information conveyed to me by other law enforcement officials, information related by witnesses, review of physical evidence obtained during the investigation, and a review of records including business records, patient records, and Medicare and Medicaid claims data. Unless otherwise indicated, all statements related herein are related in substance and in part, and are not verbatim. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact observed by me or known to law enforcement regarding this investigation.

#### **LEGAL PRINCIPLES**



## **A. UNLAWFUL DISTRIBUTING OR DISPENSING OF CONTROLLED SUBSTANCES UNDER TITLE 21**

7. The Controlled Substances Act (“CSA”) governs the manufacture, distribution, and dispensing of controlled substances in the United States. *See* 21 U.S.C. § 801 *et seq.* It is a federal offense for any person to knowingly or intentionally distribute or dispense a controlled substance except as authorization by law. *See* 21 U.S.C. § 841(a)(1) (“Section 841(a)(1)”). It is similarly a federal offense to conspire to violate Section 841(a)(1). *See* 21 U.S.C. § 846.

8. Medical professionals, including physicians, registered with the Attorney General are authorized under the CSA to write prescriptions for, or to otherwise distribute or dispense, controlled substances, as long as they comply with requirements under their registration. Title 21, United States Code, Section 822(b). Such medical professionals are then assigned a registration number with the DEA.

9. To comply with the terms of their registration, medical professionals cannot issue a prescription for a controlled substance unless it is “issued for a legitimate medical purpose by an individual practitioner acting in the usual course of his professional practice.” 21 C.F.R. 1306.04(a). Section 1306.04(a) provides that:

A prescription for a controlled substance to be effective must be issued for a legitimate medical purpose by an individual practitioner acting in the usual course of his professional practice. The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner, but a corresponding responsibility rests with the pharmacist who fills the prescription. An order purporting to be a prescription issued not in the usual course of professional treatment or in legitimate and authorized research is not a prescription within the meaning and intent of Section 309 of the Controlled Substances Act (Title 21, United States Code, Section 829) and the person knowingly filling such a purported prescription, as well as the person issuing it, shall be subject to the penalties provided for violations of the provisions relating to controlled substances.

10. Put another way, a medical professional violates Section 841(a)(1) when he or she knowingly issues or fills a prescription for a controlled substance that is *not* for a legitimate medical purpose or within the usual course of professional practice. Analyzing this issue often turns on the facts of a particular case. There are nonetheless red flags that are indicative of prescriptions that are not issued for a legitimate medical purpose. Certain of these red flags are discussed below.

11. The CSA and its implementing regulations set forth which drugs and other substances are defined by law as “controlled substances” and further assigns each drug or substance to one of five schedules (Schedule I-V), depending on the drug or substance’s potential for abuse, likelihood of physical or psychological dependency, accepted medical use, and accepted safety for use under medical supervision.

12. Schedule II drugs contain those commonly referred to as “opioids,” generally known as Oxycodone, Oxymorphone, Hydrocodone, Oxycontin, fentanyl, and morphine sulphate. These drugs are highly addictive prescription painkillers, which may lead to severe psychological or physical dependence, overdose or death. These drugs are also routinely diverted for non-legitimate medical purposes and are often sold after prescribed and abused by those seeking a euphoric feeling or “high” from the drug.

13. Schedule IV drugs include, among others, benzodiazepines, which are commonly used to treat insomnia and anxiety. There is a potential for dependence and abuse of benzodiazepines particularly by individuals with a history of substance abuse. Alprazolam (Xanax) and diazepam (Valium) are some of the most prescribed benzodiazepines and most frequently encountered benzodiazepines on the illicit market.

14. Prescribing or issuing prescriptions for benzodiazepines and Schedule II opioids is frequently *not* for a legitimate medical purpose or outside the usual course of professional practice. Prescribing and issuing these two medications around the same time compounds the patient's risk of overdose and death from the prescribed drugs, by five (5) times. Moreover, there is a significant diversion risk of prescribing or issuing these drugs around the same time. A benzodiazepine serves as a "potentiator" for the opioid's euphoric effect and increases the "high" a user may obtain from opioid and is often sought for this non-legitimate medical purpose.

15. On March 16, 2016, the Centers for Disease Control and Prevention ("CDC") issued CDC Guidelines for Prescribing Opioids for Chronic Pain. In that guidance, the CDC warned that medical professionals should avoid prescribing opioids and benzodiazepines concurrently whenever possible because of the risk of potentially fatal overdose.

16. On August 31, 2016, the U.S. Food and Drug Administration ("FDA") issued a Boxed Warning, its strongest warning, to the drug labeling of prescription opioids and benzodiazepines. The FDA specifically warned that combined use of opioids and benzodiazepines depress the central nervous system and results in serious side effects, such as slowed or difficult breathing and death. The FDA because of this harm warned health care professionals to limit prescribing opioids with benzodiazepines and cautioned that such medications should only be prescribed together for those patients for who alternative treatment options are inadequate.

## **B. HEALTHCARE FRAUD UNDER TITLE 18**

17. 18 U.S.C. § 1347 prohibits, among other things, knowingly and willfully executing or attempting to execute a scheme or artifice to defraud a health care benefit program in connection

with the delivery of or payment for health care benefits, items or services. Section 1349 prohibits conspiracy to commit healthcare fraud.

18. Medicare is a health care benefit program for purposes of Section 1347 and as defined by 18 U.S.C. Section 24(b). The Medicare Program (“Medicare”) is a federal health care program providing benefits to persons who are over the age of 65 or disabled. Medicare is administered by the United States Department of Health and Human Services (“HHS”) through its agency, the Centers for Medicare & Medicaid Services (“CMS”). Individuals who receive benefits under Medicare are referred to as Medicare beneficiaries.

19. Healthcare providers that provide services to Medicare beneficiaries are required to enroll in Medicare and receive a provider number. Part of the enrollment process requires that the healthcare providers certify that they understand and will abide by the federal laws and regulations governing their participation in Medicare, including a specific understanding of the Anti-Kickback Statute, 42 U.S.C. § 1320a-7(b).

20. A health care provider that receives a Medicare provider number is able to file claims with Medicare to obtain reimbursement for services provided to beneficiaries. A Medicare claim is required to set forth, among other things, the beneficiary’s name and Medicare information number, the services that were performed for the beneficiary, the date the services were provided, the cost of the services, and the name and identification number of the physician or other health care provider that ordered the services.

21. Medicare pays for certain prescription drugs for beneficiaries, what is commonly referred to as “Part D.” To submit claims on behalf of Medicare beneficiaries, pharmacies contract with Medicare Part D plans. CMS regulations require that all subcontracts between Part D Plan Sponsors and downstream entities contain language obligating the pharmacy to comply with all



applicable federal laws, regulations, and CMS instructions, including the CSA. *See* 42 C.F.R. § 423.505(i)(4)(iv).

22. Medicare similarly requires of its providers, among other things, that all drugs prescribed or issued be medically necessary, comply with federal law, and be for a legitimate medical purpose and in the usual course of professional practice. *See also* 42 U.S.C. § 1395y. Claims that do not comply with these requirements, and others, are false and fraudulent claims and subject the provider to prosecution under Section 1347.

23. TennCare is Tennessee's Medicaid program and is administered pursuant to Title XIX of the Social Security Act. TennCare is also health care benefit program for purposes of Section 1347 and as defined by 18 U.S.C. Section 24(b).

24. TennCare is a joint program between the State of Tennessee and the United States of America, with approximately thirty (30) percent of the funding coming from the State of Tennessee and the remaining approximate seventy (70) percent coming from the United States Federal Government. TennCare serves indigent people who cannot afford health care insurance and uninsured or uninsurable people. Individuals who receive benefits under TennCare are referred to as recipients or beneficiaries.

25. Similar to Medicare, medical providers must enroll with TennCare to become a provider. An accepted provider may then bill to, and receive payment from, TennCare for medical services and items provided to recipients. The Bureau of TennCare contracts with private insurance companies to provide insurance services to eligible persons ("enrollees"). Each of these private insurance companies is referred to as a managed care company ("MCC"). Each MCC contracts with medical service providers to render services to the enrollees. The medical service providers submit claims to the MCC, on behalf of the enrollee, and receive compensation based on those

claims.

26. For TennCare pharmacy claims, the state has assumed the financial responsibility of drugs. Through the Bureau of TennCare, the state contracts with a “Pharmacy Benefits Manager” (“PBM”), which actually pays the pharmacies. TennCare’s PBM is called Magellan. For each drug, the PBM processes and reimburses pharmacy providers for all claims from TennCare enrollees. TennCare, through the PBM, pays funds directly to retail pharmacies that in turn dispense prescription medications to the TennCare recipient. The TennCare prescription program operates on a claim-for-service basis.

27. TennCare requires of its providers, among other things, that all drugs prescribed or issued be medically necessary, comply with federal law, and be for a legitimate medical purpose and in the usual course of professional practice. *See* Tenn. Comp. R. & Regs. 1200-13-16-.05(1)(a)-(c); *see also* 42 U.S.C. § 1395y. Claims that do not comply with these requirements, and others, are false and fraudulent claims and subject the provider to prosecution under Section 1347.

### **C. THE ANTI-KICKBACK STATUTE UNDER TITLE 42**

28. Title 42, United States Code, Section 1320a-7(b)(2)(A), prohibits the paying and receiving illegal remuneration, that is, knowingly and willfully offering, paying and receiving any remuneration (including any kickback, bribe or rebate) directly or indirectly, overtly or covertly, in cash or in kind to any person or from any person or entity to induce such person to refer an individual or as an inducement to refer individuals for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a federal program.

29. Claims submitted to federal health care programs while also knowingly and

willfully paying or receiving kickbacks or bribes in return for referring federal health care patients for medical services or items, is a violation of the Anti-Kickback Statute, under Title 42.

## PROBABLE CAUSE OF FEDERAL VIOLATIONS

### *Relevant Individuals and Entities*

30. Affiant believes that GHEARING, and co-conspirators known and unknown, have unlawfully distributed and dispensed prescriptions for controlled substances. GHEARING, according to the investigation, has repeatedly and systematically distributed and dispensed controlled substances for no legitimate medical purpose and outside the usual course of professional practice.

31. GHEARING is a physician licensed with the State of Tennessee as of on or about January 24, 1986. GHEARING, according to the State of Tennessee, specializes in family medicine. GHEARING is a provider with both Medicare and TennCare.

32. Investigators opened a criminal investigation of GHEARING based on his prescriptions that are indicative of issuing controlled substances for no legitimate medical purpose and outside the usual course of professional practice.

33. GHEARING, according to a review of Tennessee's Controlled Substances Monitoring Database ("CSMD"), has prescribed numerous controlled substances in combinations that indicate prescriptions for no legitimate medical purpose and outside the usual course of professional practice. From in or around December 2015 to in or around November 2018, GHEARING, according to CSMD, prescribed the following controlled substances:

Drug Name	Drug Class	Number of Unique RXs	Number of RXs Including Refills	Number of Pills
OXYCODONE HCL / ACETAMINOPHEN	CII	2,763	2,798	134,670
ALPRAZOLAM	CIV	1,735	2,862	190,200
CLONAZEPAM	CIV	1,095	1,752	107,354
TRAMADOL HCL	CIV	768	848	60,041
CARISOPRODOL	CIV	459	528	22,176
HYDROCODONE BITARTRATE ACETAMINOPHEN	CII	437	442	29,463
GABAPENTIN	CV	429	852	95,523
DIAZEPAM	CIV	291	405	26,069

34. In my training and experience, this prescription history is indicative of prescriptions that are not for a legitimate medical purpose and outside the scope of professional practice.



GHEARING, as discussed herein, prescribes opioids with numerous potentiators, such as benzodiazepines (Alprazolam, Clonazepam, Diazepam) and Carisoprodol (a purported muscle relaxer). Prescriptions for potentiators and opioids, as discussed above, both increase the risk of overdose and death to patients and often sought to increase the “high” for opioids. Prescribing these drugs consistently together is, based on my training and experience, indicative of prescriptions issued for no legitimate medical purpose and outside the usual course of professional practice.

35. Patients of GHEARING, according to CSMD data, fill more prescriptions at Anderson Hometown Pharmacy, LLC (“Anderson Hometown”), than any other single pharmacy. Anderson Hometown is located in the same building as the TARGET LOCATION. Anderson Hometown Pharmacy pays GHEARING purported rent for the space of Anderson Hometown. Because GHEARING is Anderson Hometown Pharmacy’s top prescriber for prescriptions dispensed, receives payment from federal health care programs for those prescriptions, and pays GHEARING rent, this relationship suggests a possible unlawful financial relationship in violation of the Anti-Kickback Statute.

### **Criminal Investigation**

#### *GHEARING’s Prescriptions for the “Holy Trinity”*

36. GHEARING, according to CSMD, distributes and dispenses prescriptions for the “Holy Trinity,” a drug cocktail that is sought out for diversion and poses an extremely high risk of overdose and death for patients. The “Holy Trinity” consists of prescriptions for the following drugs: a muscle relaxant (such as Carisoprodol, sold under the name Soma), a benzodiazepine (such as Xanax), and a Schedule II opioid (such as oxycodone). Affiant is not aware of a legitimate medical purpose for these drugs to be prescribed to one patient in or around the same

time. The “Holy Trinity” is a well-known drug cocktail of abuse among medical professionals and law enforcement.

37. GHEARING, according to CSMD data, between June 2016 and November 2018, has prescribed the “Holy Trinity” to approximately twenty-seven (27) patients. These patients, according the same data, have filled approximately eighty-nine (89) prescriptions for the “Holy Trinity.” GHEARING’s practice of prescribing patients the “Holy Trinity” is a red flag for prescribing controlled substances for no legitimate medical purpose and outside the usual course of professional practice.

*GHEARING’s Prescriptions for Opioids combined with Benzodiazepines*

38. As noted above, individuals who divert prescription drugs often seek out prescriptions of benzodiazepines and opioids because of the potentiating effect the benzodiazepine has on the “high” of the opioid. Such drug combinations also pose a significant risk of overdose and death to the patient because of respiratory depression, as discussed above and as cautioned by the FDA and CDC.

39. GHEARING, according to CSMD data, between February 2016 and November 2018, has prescribed benzodiazepines around the same time as opioids to approximately two hundred and fifty (250) patients. These patients, according the same data, have filled approximately 1,100 prescriptions for opioids around the same time as a benzodiazepine. Prescribing patients the combination of a benzodiazepine and an opioid is a red flag that GHEARING is prescribing controlled substances for no legitimate medical purpose and outside the usual course of professional practice.

*GHEARING's Prescriptions to a Confidential Source*

40. On December 20, 2018, a confidential source ("CS") visited the TARGET LOCATION for a purported medical visit with GHEARING. Following that visit, GHEARING, Affiant believes, prescribed the CS a controlled substance, which Affiant believes to be not for a legitimate medical purpose and outside the usual course of professional practice. CS's visit to the TARGET LOCATION and CS's interactions with GHEARING was recorded on an audio/visual device.

41. CS, who was a previous patient of GHEARING, visited GHEARING complaining of pain in CS's shoulder. CS told GHEARING that CS injured CS's left shoulder on Monday, December 17. CS's injury was fictional.<sup>1</sup> GHEARING physically examined the CS's shoulder for approximately three minutes. GHEARING concluded that CS had arthritis in CS's shoulder and probably had a flare up. GHEARING told CS that he would give CS a prescription for pain and one for arthritis. CS asked GHEARING if he could "get something for the pain." GHEARING confirmed that he would write CS something (a prescription) for pain for just a few days and something (a prescription) for arthritis. GHEARING confirmed later in the visit that he sent in "pain pills" and something for arthritis for CS.

42. Affiant believes, based on his training and experience, that GHEARING's medical visit with CS was outside the usual course of professional practice for several reasons. First, GHEARING performed only a quick examination of CS's shoulder. Second, GHEARING

---

<sup>1</sup> Based on Affiant's training and experience, individuals seeking prescriptions for controlled substances frequently complain of non-existent injuries or exaggerate the severity of real injuries to induce physicians to prescribe controlled substances to be abused. Such actions are well known both within the medical community and law enforcement. Prescribers acting within the usual course of professional practice must be vigilant in guarding against this reality when prescribing controlled substances.

prescribed opioids to CS without trying other non-addictive treatments first, such as over-the-counter medication. Third, GHEARING did not counsel CS about the risks of opioids or even discuss with CS what opioids he was prescribing to CS. Fourth, GHEARING did not check the prescription history or CSMD of CS before prescribing opioids. Had GHEARING done so, he would have seen that CS was prescribed buprenorphine by another physician, which is generally a medication taken by those addicted to opioids. Further, GHEARING sent CS's prescriptions to Anderson Hometown. Anderson Pharmacy refused to fill GHEARING's prescription on behalf of CS for this reason. Neither CS nor Affiant know what "pain pills" GHEARING prescribed to CS because GHEARING sent CS's prescription electronically to Anderson Hometown, did not give CS a hardcopy of that prescription, and did not discuss the prescription itself with CS. Affiant believes that GHEARING nonetheless prescribed a controlled-substance opiate to CS because otherwise Anderson Hometown would not have refused to fill CS's prescription on the basis of CS's buprenorphine history.

*GHEARING's Prescriptions to an Undercover Agent ("UC"): January 8, 2019*

43. UC visited the TARGET LOCATION for a purported medical visit with GHEARING. During the visit, GHEARING prescribed controlled substances to UC outside the usual course of professional practice. UC paid GHEARING \$75 for this visit, and others, because UC purported to not have insurance. Each prescription from GHEARING to UC, based on Affiant's training and experience and as discussed below, is outside the usual course of professional practice.

44. On January 8, 2019, the UC visited the TARGET LOCATION for a purported medical visit with GHEARING. Once inside the TARGET LOCATION, UC explained to an unidentified office worker that UC was there to see GHEARING for shoulder pain. UC's injury



was fictional. UC later explained to GHEARING how UC's shoulder hurt all of the time and how UC had tried ibuprofen and Tylenol but without benefit anymore. GHEARING examined UC's shoulder for approximately two minutes. GHEARING told UC that UC probably had arthritis in the joint and that he would prescribe something good for arthritis and something mild for the pain.

45. UC told GHEARING that UC knew nothing was broken or messed up or anything. UC then told GHEARING how UC is unsure whether UC should say anything, but how UC has taken medication from a friend and further how the medication "helps." Later in the conversation, UC told GHEARING that a buddy gave UC "hydros" and how UC took eight of those, which worked good. GHEARING again did not respond to this statement or otherwise ask follow up questions.

46. GHEARING told UC that he would prescribe UC something for arthritis and a "pain pill." UC asked about the pain pills. GHEARING noted that he wrote some stuff and that UC could take it if UC is "dying of pain." The pain pills, according to GHEARING, were not the secret and the thing is to figure out how to fix UC's injury. GHEARING informed UC that he planned to give UC a shot if the injury did not get better in a month or so. GHEARING told UC that UC could fill UC's prescriptions at Anderson Hometown next door and told UC to come back in three or four weeks.

47. On January 8, 2019, GHEARING prescribed UC twelve (12) pills of Oxycodone-Acetaminophen (5-325), a Schedule II controlled substance, and thirty (30) pills of Meloxicam, which not a controlled substance. UC filled these prescriptions at Anderson Hometown.

48. Affiant believes, based on his training and experience, that GHEARING prescribed UC controlled substances outside the usual course of professional practice for several reasons.

First, GHEARING performed only a cursory examination of UC's complained injury. Second, GHEARING ignored obvious red flags of diversion that UC brought to GHEARING's attention, including taking controlled substances without a prescription and referring to such medication as "hydros," a slang or "street" term for hydrocodone that is associated with diversion. Despite knowing that UC took controlled substances without a prescription, GHEARING still prescribed UC controlled substances and made no known effort to check the UC's prescription history. Third, GHEARING did not explain the risks of the opioids to UC or otherwise provide UC any information about the controlled substances other than to take the pills if UC was "dying of pain." Fourth, GHEARING prescribed UC a controlled substance during UC's first visit with him.

*GHEARING's January 14, 2019 Prescriptions to an Undercover Agent ("UC")*

49. On January 14, 2019, UC returned to the TARGET LOCATION for a follow-up visit with GHEARING, which was recorded on an audio device. During the visit, GHEARING prescribed controlled substances to UC outside the usual course of professional practice.

50. UC told GHEARING that UC's shoulder was a little better. UC explained to GHEARING that she noticed a big difference in UC's pain levels once she ran out of the pain pills. GHEARING briefly examined UC's shoulder. GHEARING told UC that he did not want UC to take the pain pills very much, just to take them until UC started moving UC's shoulder and until the other "stuff" could get into UC's system. GHEARING recommended that UC do jumping jacks to loosen up UC's shoulder. After an unrelated discussion, GHEARING told UC that he "sent in" pain pills and an unrelated medication for UC. GHEARING told UC to move around and that he would consider an x-ray or shot if it does not get better.

51. UC asked GHEARING to prescribe Xanax (a benzodiazepine) to UC. GHEARING told UC that it's so easy to get addicted to Xanax and how everyone is anxious at times. UC told

GHEARING that UC is already taking Xanax because UC gets them from Ms. Gilbert. GHEARING asked if Ms. Gilbert is a nurse. UC told GHEARING that Ms. Gilbert is a friend. GHEARING responded that the problem with Xanax is that they are so addictive and how once someone gets on Xanax it is hard to get off. GHEARING referred UC to Dale Hollow Mental Health if UC wants those medications and told UC that he will not do that (prescribe Xanax) just yet. UC asked GHEARING about the medication that he sent in. GHEARING told UC that he sent in the “same number” and not to take the medication unless UC has to – “like crying” in pain. GHEARING told UC that he does not want UC to take too much.

52. On January 14, 2019, GHEARING prescribed UC twelve (12) pills of Oxycodone-Acetaminophen (5-325), a Schedule II controlled substance, and an unrelated medication. UC filled this prescription at Anderson Pharmacy.

53. Affiant believes for the reasons stated above that GHEARING’s prescription was outside the usual course of professional practice. GHEARING notably prescribed UC controlled substances after having direct conversations with UC about UC taking another controlled substance from a friend (diversion).

*GHEARING’s January 22, 2019 Prescriptions to UC*

54. On January 22, 2019, UC returned to the TARGET LOCATION for a follow-up visit with GHEARING, which was recorded on an audio/visual device. During the visit, GHEARING prescribed UC controlled substances outside the usual course of professional practice.

55. GHEARING again quickly examined UC’s shoulder and informed UC that he would get UC an X-ray and possibly an injection. UC asked GHEARING if UC could make the medicine last longer. GHEARING replied that he usually does not give pain medicines, just once

in a while. GHEARING stated that he does not want UC to be on any pain medication and wants to fix UC's shoulder. UC persisted in requests for additional pain medicine. GHEARING described how he would like to have UC take an x-ray to determine what is going on with UC's shoulder and explained how he wanted UC to get a shot in UC's shoulder, an offer which UC rejected.

56. On January 22, 2019, GHEARING prescribed UC twelve (12) pills of Oxycodone-Acetaminophen (5-325), a Schedule II controlled substance. UC filled this prescription at Anderson Pharmacy. Affiant believes that GHEARING's prescription was again outside the usual course of professional practice for the above-cited reasons.

*GHEARING's January 31, 2019 Prescriptions to UC*

57. On January 31, 2019, UC returned to the TARGET LOCATION for another visit with GHEARING. During the visit, GHEARING again prescribed UC controlled substances outside the usual course of professional practice. This visit was recorded on an audio/visual device and is summarized below.

58. UC and GHEARING discussed the results of UC's x-ray for UC's shoulder. GHEARING described how UC has arthritis in UC's shoulder. GHEARING described how he "didn't know what was wrong with [UC] before."

59. UC and GHEARING discussed UC's prescriptions. UC tells GHEARING that the pain pills worked better than the anti-inflammatory medicine GHEARING also prescribed. GHEARING told UC that the pain pills just cover up the pain and recommended that UC get a shot in UC's shoulder, which would lessen the pain for about two weeks.

60. UC told GHEARING that GHEARING needed to write UC a prescription for "Valium or something" because of UC's feelings after hearing UC has arthritis. GHEARING

responded that he can write UC something for anxiety. GHEARING told UC that the news about arthritis is not terrible and how it is not like cancer. GHEARING told UC that it is unusual for UC to have arthritis in UC's shoulder without something bad happening to UC. GHEARING then told UC that he sent in UC prescriptions for pain and Xanax.

61. On January 31, 2019, GHEARING prescribed UC twelve (12) pills of Oxycodone-Acetaminophen (5-325), a Schedule II controlled substance, and sixty (60) pills of Alprazolam (Xanax), a Schedule IV controlled substance. UC filled this prescription at Anderson Pharmacy. Affiant believes that GHEARING's prescriptions were again outside the usual course of professional practice. Notably, GHEARING prescribed UC Xanax after UC told GHEARING what he needed to prescribe. This behavior, according to Affiant's training and experience, is consistent with drug-seeking behavior. Further, GHEARING had previously warned UC about the significant risks of addiction associated with Xanax, as described above. Nonetheless, GHEARING prescribed UC what he knows to be a highly addictive drug after UC's specific request for the drug and in conjunction with a Schedule-II opioid. Such conduct is outside the usual scope of professional practice and not for a legitimate medical purpose.

62. During the UC visits described above, GHEARING did not request urinalysis screening of the UC to determine what controlled substances the UC was taking. This is a practice normally performed by providers prescribing controlled substances to determine if a patient takes medications as prescribed, diverts the medications, or is already taking other legal or illegal substances. The absence of GHEARING requesting urinalysis is a sign that GHEARING's conduct is outside the usual course of professional practice and not for a legitimate medical purpose.



**PROBABLE CAUSE TO BELIEVE EVIDENCE OF CRIMES, AMONG OTHER THINGS, WILL BE FOUND AT THE TARGET LOCATION**

63. Affiant believes that evidence, records, instrumentalities and other evidence of the above-referenced crimes will be found at the TARGET LOCATION.

64. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires covered entities, such as pharmacies billing Medicare and Medicaid (TennCare), to retain required documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is longer. HIPAA requirements preempt state laws if they require shorter periods. *See* 45 CFR § 164.316.

65. Under Tennessee statute, providers submitting claims to TennCare, like GHEARING, must maintain records for a minimum of five (5) years after the date on which payment was received. *See* Tenn. Code Ann. § 71-5-2602.

66. UC and CS, as noted above, both visited with GHEARING at the TARGET LOCATION on numerous occasions. During each visit, GHEARING and his employees at the TARGET LOCATION collected information about the UC and CS regarding their purported medical condition. Affiant believes, based on these visits and his training and experience, that GHEARING keeps and maintains records relating to his practice at the TARGET LOCATION.

67. In my training and experience, and on my consultation with other law enforcement officers experienced in investigations regarding unlawful distribution of controlled substances, health care fraud, financial fraud, and money laundering, persons involved in the unlawful distribution of controlled substances, including physicians, often keep controlled substances, proceeds of sales, records of transactions and other records within their businesses or within ready access. The documentary records and ledgers remain at the place of business.

68. Persons involved in the unlawful distribution of controlled substances and health care fraud, purchase real estate, vehicles, or other expensive items using proceeds of illicit activity and maintain records, documents, or materials, evidencing such purchases in their business locations and other locations.

69. It is common knowledge within the law enforcement community that controlled-substances transaction records, books, account ledgers, payments, or notes and other evidence of financial transactions relating to obtaining, transferring, and spending substantial sums of money that result from engaging in illicit activities are often maintained at or in the target's business location and other locations.

70. Persons involved in the unlawful distribution of controlled substances and health care fraud, including pharmacists, often retain personal and business notes, letters, and correspondence relating to their prescription orders at or in their businesses and other locations.

71. Physicians routinely maintain files in their medical offices for patients who visit such locations. From my training and experience, I know that physicians keep these types of patient records and controlled-substance records on paper, electronically on computers, or in other electronic formats.

72. I expect that officers will find evidence of controlled substances distribution and health care fraud within the TARGET LOCATION in the form of prescriptions for controlled substances, United States currency, medical records (in any format including paper records and electronic records), signature logs, billing logs, payment records, prescriptions, patient files with fictitious documentation, invoices, computers, computer servers and external hard drives, as described more particularly in ATTACHMENT B, hereby incorporated by reference.

73. Your Affiant also knows that individuals and businesses engaging in financial fraud related to the above-referenced crimes frequently maintain records of their financial transactions and these records can be either in the form of a formal set of books and records, or informal notations, and can be maintained as physical documents and/or as digital data stored on computers and related computer/electronic storage media at their place of business. Individuals and their business entities generally retain their bank account records, Secretary of State filings, corporate records, income tax returns, employment tax returns, financial statements, loan documents, records relating to the purchase, sale, and improvement of real property, contracts, and other documents reflecting a financial interest in one's business entities at their businesses and/or personal residence. It is the ordinary and customary practice of individuals and businesses engaging in healthcare fraud, related financial fraud, and unlawful distribution of controlled substances to maintain financial records of all income and expenses, in addition to accounting records, payroll records, bank statements, deposit items and offsets, loan documents, balance sheets, financial statements, inventory sheets, register tapes, client lists, accounts receivable ledgers, and customer lists. These records are maintained in order to provide the business owner or another party with the necessary documentation for the preparation and filing of corporate returns, partnership returns, or the Schedule C, for determining net income to be reported on an individual income tax return; state sales and use tax reporting; state and federal wage and employment tax returns; and for adherence to local, state and federal regulatory guidelines.

74. Based on my knowledge and experience, your Affiant knows individuals and businesses that commit unlawful distribution, healthcare fraud, financial fraud, maintain records of the financial transactions at their business, and your Affiant is requesting to search TARGET

LOCATION for evidence of violations of the Controlled Substances Act, health care fraud, and related financial crimes, as described in this affidavit.

**MANNER AND MEANS OF EXECUTING THE SEARCH OF THE TARGET**

**LOCATION**

*Electronic Medical Records/Electronic Evidence: Technical Terms*

75. Based on your Affiant's training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

76. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

77. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

78. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including,

but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

79. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

80. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or

wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

81. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

82. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or



code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

83. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

84. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- a. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- b. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based

dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

- c. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.
- d. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

85. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized

party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

*Computers, Electronic Evidence, And Forensic Analysis*

86. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the TARGET LOCATION, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the TARGET LOCATION, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

- a. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, individuals and entities who provide medical services regularly with Medicaid, Medicare, private insurance companies, and vendors, not only use computers to access websites and to communicate with others online, but they also store documents and records on computer hard drives and other electronic storage media devices. These documents and records can include logs of online “chats”; e-mail correspondence; contact information of individuals, including telephone numbers, e-mail addresses, identifier for instant messaging and social media accounts; financial and personal identification data, including bank account numbers, credit card numbers, Medicare and Medicaid identification numbers and names, addresses, telephone numbers, and social security numbers of other individuals.
- b. Individuals and entities who provide medical services, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.
- c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools.

When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

87. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices,

I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

- a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the



sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.
- c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.
- f. I know that when an individual uses a digital device to commit the above referenced violations, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

*Methods to be used to Search Digital Devices*

88. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.
- b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.
- c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the

device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

- d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches

because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

- e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by

individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

- f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

89. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the TARGET LOCATION.

- a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:
  - i. Upon securing the TARGET LOCATION, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal



Procedure, seize any digital devices, within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the TARGET LOCATION. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

- ii. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of

language contained in such storage areas exist that are related to the subject matter of the investigation.

- iii. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.
- iv. The TARGET LOCATION is a functioning medical office that conducts legitimate business. The seizure of the Company’s digital devices may limit GHEARING’s ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what digital devices must be seized or copied, and what digital devices need not be seized or copied. Where appropriate, law enforcement personnel executing the warrant will copy data, rather than physically seize digital devices, to reduce the extent of disruption. If employees of GHEARING so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the GHEARING’s legitimate business. If, after

inspecting seized digital devices, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve evidence, the government will return it.

90. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

91. Technical requirements. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices such as desktop computers, laptop computers, or portable storage devices, may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

92. Examination requirements. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

93. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises of the TARGET LOCATION, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

### **CONCLUSION**

94. I submit that this affidavit supports probable cause for a warrant to search the TARGET LOCATION, more particularly described in Attachment A and seize the items described in Attachment B. Your Affiant believes, based on the facts set forth above, that there is probable cause to search the TARGET LOCATION for evidence of crimes in violation of the Controlled Substances Act, including but not limited to, Title 21, United States Code, Sections 841 (Illegal Distribution and Dispensing of Controlled Substances) and 846 (Conspiracy to Distribute and Dispense Controlled Substances), and violations of Title 18 United States Code, Sections 1347 (Health Care Fraud) and 1349 (Conspiracy to Commit Healthcare Fraud), and 42

U.S.C. § 1320a-7(b) (Anti-Kickback Statute). Your Affiant believes that examination of materials obtained in the search will produce admissible evidence that GHEARING dispensed and distributed highly addictive controlled substances to patients for other than a legitimate medical purpose and outside the usual course of his professional practice. Your Affiant also believes that examination of the materials obtained in the search will produce admissible evidence that GHEARING caused to be submitted claims to federal healthcare programs for medications that are not medically necessary. Your Affiant also believes GHEARING committed these crimes for profit, and examination of financial records maintained will produce admissible evidence of financial crimes, as set forth herein.

95. I respectfully request that the Court issue a search warrant for the locations described herein and pictured in Attachment A, authorizing the seizure and search of items listed in Attachment B of the search warrant.